安心社会の基盤を構築する情報セキュリティ技術

総合理工学部　准教授　黄　緒平

生成系AIが脚光を浴び、音声合成や画像・動画の高速処理など、機械学習の発展により、声紋や顔など公共の場で採取可能な他人の生体特性を悪用し、他者になりすますことが容易になった。声や映像を模倣する技術は日進月歩で進化し、世界を席巻する勢いで飛躍的に発展している。そのため、データの真贋判定や話者の正確な識別を行う技術がますます重要になっている。

黄研究室では、安心・安全な社会基盤を構築するため、情報セキュリティの三要素である完全性、可用性、および機密性に関する研究を深めている。特に、改ざん検出やなりすましの特定が可能な、可逆的で頑健な電子透かし技術の開発に注力している。また、マルウェアの観測および数理モデルに基づく解析を通じて、不正アクセスやサイバー攻撃の挙動を調査・研究している。更に、ヘルスケア生体情報の解析技術や、プライバシー保護技術の研究にも取り組んでいる。